### WRT300N Wireless Router Configuring

Wireless Security

Linksys wants to make wireless networking as safe and easy for you as possible. The current generation of

Linksys products provide several network security features, but they require specific action on your part for

implementation. So, keep the following in mind whenever you are setting up or using your wireless network.

Security Precautions

The following is a complete list of security precautions to take (at least steps 1 through 5 should be followed):

1. Change the default SSID.

2. Disable SSID Broadcast.

3. Change the default password for the Administrator account.

4. Enable MAC Address Filtering.

5. Change the SSID periodically.

6. Use the highest encryption algorithm possible. Use PSK if it is available. Please note that this may reduce your

network performance.

7. Change the WEP encryption keys periodically.

For information on implementing these security features, refer to “Chapter 5: Configuring the Wireless-N

Broadband Router.”

Security Threats Facing Wireless Networks

Wireless networks are easy to find. Hackers know that in order to join a wireless network, wireless networking

products first listen for “beacon messages”. These messages can be easily decrypted and contain much of the

network’s information, such as the network’s SSID (Service Set Identifier). Here are the steps you can take:

Change the administrator’s password regularly. With every wireless networking device you use, keep in

mind that network settings (SSID, WEP keys, etc.) are stored in its firmware. Your network administrator is the

only person who can change network settings. If a hacker gets a hold of the administrator’s password, he, too,

can change those settings. So, make it harder for a hacker to get that information. Change the administrator’s

password regularly.

Security Threats Facing Wireless Networks

Wireless-N Broadband Router

SSID. There are several things to keep in mind about the SSID:

1. Disable Broadcast

2. Make it unique

3. Change it often

Most wireless networking devices will give you the option of broadcasting the SSID. While this option may be

more convenient, it allows anyone to log into your wireless network. This includes hackers. So, don’t broadcast

the SSID.

Wireless networking products come with a default SSID set by the factory. (The Linksys default SSID is “linksys”.)

Hackers know these defaults and can check these against your network. Change your SSID to something unique

and not something related to your company or the networking products you use. Change your SSID regularly so that any hackers who have gained access to your wireless network will have to

start from the beginning in trying to break in.

MAC Addresses

Enable MAC Address filtering. MAC Address filtering will allow you to provide access to only

those wireless nodes with certain MAC Addresses. This makes it harder for a hacker to access your network with

a random MAC Address.

WEP Encryption

Wired Equivalent Privacy (WEP) is often looked upon as a cure-all for wireless security

concerns. This is overstating WEP’s ability. Again, this can only provide enough security to make a hacker’s job

more difficult.

There are several ways that WEP can be maximized:

1. Use the highest level of encryption possible

2. Use “Shared Key” authentication

3. Change your WEP key regularly

PSK

PSK is stronger than WEP encryption, and PSK2 has stronger encryption than PSK. PSK and PSK2 gives you

a choice of two encryption methods: TKIP (Temporal Key Integrity Protocol), which incorporates Message Integrity

Code (MIC) to provide protection against hackers, and AES (Advanced Encryption System), which utilizes a

symmetric 128-Bit block data encryption. (AES is stronger than TKIP.)

PSK-Enterprise and PSK2-Enterprise use a RADIUS (Remote Authentication Dial-In User Service) server for

authentication. RADIUS uses a RADIUS server and WEP encryption.

IMPORTANT: Always remember that each device

in your wireless network MUST use the same

security method and key, or else your wireless

network will not function properly.

Appendix B: Wireless Security 65

Security Threats Facing Wireless Networks

Wireless-N Broadband Router

PSK/PSK2-Personal. Select the type of algorithm, TKIP or AES, and enter a password in the Pre-shared Key

field of 8-63 characters. Enter a Key Renewal period time between 0 and 99,999 seconds, which instructs the

Router or other device how often it should change the encryption keys.

PSK/PSK2-Enterprise. This method is PSK or PSK2 used in coordination with a RADIUS server. Enter the IP

address and port number of the RADIUS server. Then enter the key shared between the Router and its RADIUS

server. Then enter a Key Renewal period, which instructs the Router or other device how often it should

change the encryption keys.

RADIUS. This method is WEP used in coordination with a RADIUS server. Enter the IP address and port

number of the RADIUS server. Then enter the key shared between the Router and its RADIUS server. Enter the

WEP settings.

Implementing encryption may have a negative impact on your network’s performance, but if you are transmitting

sensitive data over your network, encryption should be used.

These security recommendations should help keep your mind at ease while you are enjoying the most flexible

and convenient technology Linksys has to offer.